UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
SEATTLE DIVISION

CRYSTAL LAM and NINA PHAN, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

T-MOBILE USA, INC., a Delaware corporation,

Defendant.

CASE NO. _____

CLASS ACTION COMPLAINT FOR VIOLATIONS OF:

1. **Negligence**
2. **Negligence *Per Se***
3. **Gross Negligence**
4. **Invasion of Privacy**
5. **Breach of Implied Contract**
6. **Breach of Implied Covenant of Good Faith and Fair Dealing**
7. **Unjust Enrichment**
8. **Declaratory and Injunctive Relief**
9. **California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.***
10. **California Consumer Legal Remedies Act, *Cal. Civ. Code §§ 1750, et seq.***
11. **California Consumer Privacy Act, *Cal. Civ. Code §§ 1798.100, et seq.***
12. **Hawaii Security Breach Notification Act, Haw. Rev. Stat. §§ 487N-1, *et seq.***
13. **Hawaii Unfair Practices And Unfair Competition Act, Haw. Rev. Stat. §§ 480-1, *et seq.***
14. **Hawaii Uniform Deceptive Trade Practice Act, Haw. Rev. Stat. §§ 481A-3, *et seq.***
15. **Washington Data Breach Notice Act, Wash. Rev. Code §§ 19.255.010, *et seq.***
16. **Washington Consumer Protection Act, Wash. Rev. Code Ann. §§ 19.86.020, *et seq.***

JURY TRIAL DEMANDED

Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP

TABLE OF CONTENTS

LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP

Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP

Plaintiffs, identified *infra* at Section II(A), individually and on behalf of all others similarly situated ("Plaintiffs"), bring this action against Defendant T-Mobile USA, Inc. ("T-Mobile"), seeking monetary damages, restitution, and/or injunctive relief. Plaintiffs make the following allegations upon personal knowledge and on information and belief derived from, *inter alia*, facts that are a matter of public record and investigation of their counsel.

"[A] brazen heist that could give criminals the digital keys to commit widespread online fraud." –The Wall Street Journal on the T-Mobile data breach[1]

I. NATURE OF THE ACTION

1. On August 15, 2021, *Vice's Motherboard* first reported that T-Mobile suffered a massive customer data breach. In a forum post on the dark web, someone sought to sell T-Mobile customer data, including names, dates of birth, social security numbers, driver's license/identification information, physical addresses, phone numbers, International Mobile Subscriber Identity (IMSI) numbers, international mobile equipment identity (IMEI) numbers, and subscriber identity modules (SIM).[2] The seller informed *Motherboard* that it had obtained data related to over 100 million people from T-Mobile servers.[3] "T-Mobile USA. Full customer info," the seller told *Motherboard* in an online chat. *Motherboard* reviewed samples of the data and confirmed they contained accurate information on T-Mobile customers.[4] The victims of the data breach include former, current, and prospective T-Mobile customers—essentially, anyone who applied for credit with T-Mobile regardless of whether they ultimately did business with the second largest carrier in the United States.

2. In the forum post, the seller sought six bitcoin, or around $270,000, for a subset of the data containing 30 million social security numbers and driver's license/identification information. The seller indicated that it was in the process of privately selling the rest of the data.

[1] https://www.wsj.com/articles/t-mobile-says-hackers-stole-details-on-more-than-40-million-people-11629285376

[2] IMSI and IMEI are unique numbers embedded in customer mobile devices that identify the device and the SIM card that links the customer's device to a telephone number.

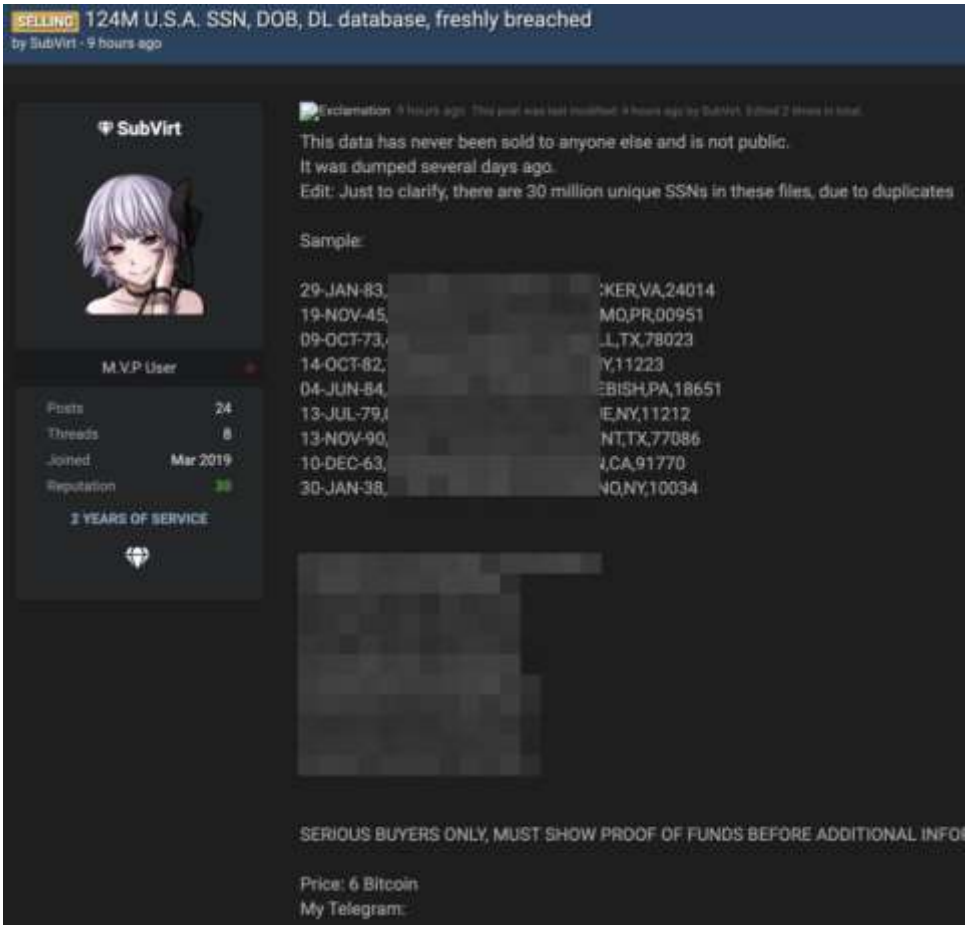
[3] https://www.vice.com/en/article/akg8wg/tmobile-investigating-customer-data-breach-100-million

[4] *Id.*

LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP

Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

The seller was unfazed that T-Mobile had closed the access point used to enter the servers because the seller had already downloaded the data locally. "It's backed up in multiple places," the seller stated.



A forum post advertising the sale of T-Mobile customer data.

3. On August 16, 2021, only a day after the article, T-Mobile confirmed that it suffered a data breach ("Data Breach"). T-Mobile called the Data Breach a "highly sophisticated cyberattack" but failed to indicate when its security team discovered the breach and how the breach occurred. An individual with the Twitter account @und0xxed claimed to know the attacker and tweeted about the attack before it was public, indicating that the attack relied on T-Mobile's lax security measures. Und0xxed said it was not involved in stealing the data but instead was responsible for finding buyers for the data. Und0xxed said the attacker used an unprotected network gateway to reach T-Mobile's backup servers, which house unencrypted information regarding customers dating back to the mid-1990s.

4. This was not T-Mobile's first data breach, but it was the largest and most serious to date. T-Mobile, with its poor security, has struggled to fight off hackers and prevent data breaches. This is the fifth data breach that T-Mobile has suffered in the past three years. In 2018, T-Mobile suffered a data breach that compromised personal information of as many as two million customers, including phone numbers, email addresses, and account numbers. In 2019, T-Mobile's email vendor suffered a data breach, revealing some T-Mobile customer and employee information.

5. In response to the data breach, T-Mobile announced it would offer two years of free identity protection services. This remedy comes too little and too late, as unauthorized individuals have already stolen and sold the personal information of tens of millions of T-Mobile customers.

6. Despite T-Mobile's representations that it provided robust security to its customers, its security was woefully inadequate. T-Mobile's unsound, vulnerable systems containing valuable data were an open invitation for an easy intrusion and simple exfiltration by cybercriminals, who were seeking to exploit the valuable nature of the information.

7. As a result of the Data Breach, Plaintiffs and the class members have suffered concrete damages, invasion of privacy, and are now exposed to a heightened and imminent risk of fraud and identity theft for many years to come. Furthermore, Plaintiffs and class members must now and in the future closely monitor their financial accounts to guard against identity theft at their own expense. Consequently, Plaintiffs and the class members have incurred, and will incur, ongoing out-of-pocket costs, including the cost of credit monitoring services, credit freezes, credit reports, and other protective measures to deter and detect identity theft, among other expenses. By this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information[5] was compromised and disclosed as a result of the

[5] As used throughout this Complaint, "Private Information" is further defined as all information exposed by the Data Breach, including all or any part or combination of name, date of birth, social security number, driver's license/ID information (including license number, state, home address, dates of issuance or expiration), and phone number.

LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP

Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

Data Breach. Accordingly, Plaintiffs bring this action against T-Mobile seeking redress for its unlawful conduct and assert claims for both common law and statutory damages.

II. PARTIES

A. Plaintiffs

8. Plaintiffs identified below bring this action on behalf of themselves and those similarly situated in a representative capacity for individuals across the United States. Despite knowing of the substantial cybersecurity risks it faced, T-Mobile, through its actions described herein, leaked, disbursed, and furnished Plaintiffs' valuable Private Information to unknown cybercriminals, thus causing them present, immediate, imminent, and continuing increased risk of harm.

9. Plaintiff **Crystal Lam** is a resident and citizen of California. Plaintiff Lam is acting on her own behalf and on behalf of others similarly situated. T-Mobile obtained and continues to maintain Plaintiff Lam's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Lam would not have entrusted her Private Information to T-Mobile had she known that it failed to maintain adequate data security. Plaintiff Lam's Private Information was compromised and disclosed as a result of the Data Breach.

10. As a result of the Data Breach, Plaintiff Lam tried to mitigate its impact, including multiple hours spent reviewing credit reports and financial account statements for any indications of actual or attempted identity theft of fraud. During this process, she discovered that she has been the subject of recent identity theft. Plaintiff Lam anticipates spending several hours a month reviewing credit monitoring reports and/or checking account statements for irregularities. The time Plaintiff Lam has spent so far on these tasks is valuable time she otherwise would have spent on other activities, including, but not limited to, work or recreation. Plaintiff Lam also felt her privacy was invaded and is suffering from emotional distress as a result of the Data Breach. Plaintiff Lam had credit monitoring before the Data Breach and continues to maintain it.

11. Plaintiff **Nina Phan** is a resident and citizen of Hawaii. Plaintiff Phan is acting on her own behalf and on behalf of others similarly situated. T-Mobile obtained and continues to

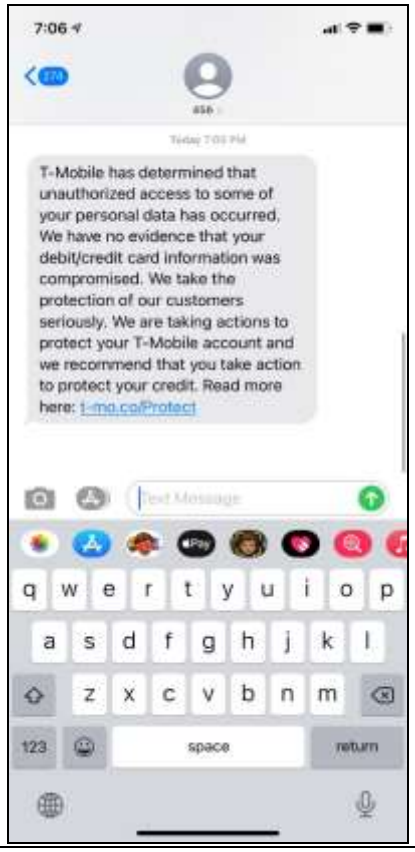
Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP

maintain Plaintiff Phan's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Phan would not have entrusted her Private Information to T-Mobile had she known that it failed to maintain adequate data security. Plaintiff Phan's Private Information was compromised and disclosed as a result of the Data Breach.

12. As a result of the Data Breach, Plaintiff Phan tried to mitigate its impact, including multiple hours spent reviewing credit reports and financial account statements for any indications of actual or attempted identity theft of fraud. Plaintiff Phan anticipates spending several hours a month reviewing credit monitoring reports and/or checking account statements for irregularities. The time Plaintiff Phan has spent so far on these tasks is valuable time she otherwise would have spent on other activities, including, but not limited to, work or recreation. Plaintiff Phan also felt her privacy was invaded as a result of the Data Breach.

13. On or around August 18, 2021, Plaintiffs received a text from T-Mobile notifying them that unauthorized third parties had improperly accessed and/or obtained their Private Information.



LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP

Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

14. While the text indicated that the Data Breach did not expose debit/credit card information, T-Mobile's investigation remains ongoing, and it is unclear how much of Plaintiffs' Private Information was exposed due to T-Mobile's conduct.

15. Based up counsel's investigation, and on information and belief, the Data Breach impacted residents and citizens of all 50 states and the District of Columbia. Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of each state and District of Columbia.

B. Defendant

16. Defendant **T-Mobile USA, Inc.** is a Delaware corporation with its principal place of business located at 12920 SE 38th Street, Bellevue, Washington 98006. T-Mobile's common stock is publicly traded on the NASDAQ under the ticker symbol "TMUS." T-Mobile is an American wireless network operator and provides wireless voice and data services in the United States. T-Mobile is the third largest wireless carrier in the United States with 104.8 million subscribers as of the end of Q2 2021. T-Mobile has annual revenues of over $40 billion.

III. JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1711, *et seq.*, because at least one member of the Class, as defined below, is a citizen of a different state than T-Mobile; there are more than 100 members of the Class; and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs.

18. This Court has personal jurisdiction over this action because T-Mobile maintains has sufficient minimum contacts with this District and has purposefully availed itself of the privilege of doing business in this District, such that it could reasonably foresee litigation being brought in this District. This Court also has diversity jurisdiction over this action. *See* 28 U.S.C. § 1332(a).

19. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because a substantial part of the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District.

IV. STATEMENT OF FACTS

A. T-Mobile Customers' Private Information Was Stolen from the Data Breach

20. T-Mobile servers contained Personally Identifiable Information ("PII") of individuals, including Plaintiffs and class members. According to the Federal Trade Commission ("FTC"), PII is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."[6]

21. According to T-Mobile, the Data Breach affected at least 48 million T-Mobile customers in the United States, including:

(a) Over 40 million former, current, or prospective customers who had previously applied for credit with T-Mobile;

(b) Approximately 7.8 million current T-Mobile postpaid customers;

(c) Approximately 850,000 active T-Mobile prepaid customers; and

(d) An undisclosed number of inactive T-Mobile prepaid customers.

22. The information compromised in the Data Breach include *at least* the following categories of PII:

(a) First and last name;

(b) Date of birth;

(c) Social security number;

(d) Driver's license/ID information;

(e) Physical address;

(f) Phone number;

(g) International Mobile Subscriber Identity (IMSI) numbers;

(h) international mobile equipment identity (IMEI) numbers; and

(i) subscriber identity modules (SIM).

---

6 *See* Federal Trade Commission Privacy Impact Assessment: Redress Enforcement Database (RED) at 3, n.3, FTC (June 2019), https://www.ftc.gov/system/files/attachments/privacy-impact-assessments/redress_enforcement_database_red_privacy_impact_assessment_june_2019.pdf.

LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP

Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

B. T-Mobile's Responsibility to Protect Its Customers' Private Information

"Telecommunications companies have a duty to protect their customers' information."

–U.S. Federal Communications Commission[7]

23. In the ordinary course of signing up for a plan with T-Mobile or financing a device through T-Mobile, consumers are required to provide Private Information, such as the categories of PII described, *supra*, for T-Mobile to run a credit check. T-Mobile is responsible for collecting, storing, maintaining, and securing this Private Information. This information is valuable and requires someone to provide security; without this Private Information, T-Mobile cannot determine whether to enter into a service contract with or providing financing for a device to a consumer.

24. T-Mobile owed Plaintiffs and class members a duty to safeguard their Private Information based on the promises that it made to its customers to safeguard data as well as the disclosures that it made in its data security policies and privacy policies. T-Mobile voluntarily undertook efforts to keep that data secure as part of its business model and thus owes a continuing obligation to Plaintiffs and class members to keep their Private Information secure.

25. T-Mobile also owed a duty to safeguard Private Information given that it was on notice that it was maintaining highly valuable data, for which T-Mobile knew there was a risk that it would be targeted by cybercriminals. T-Mobile knew of the extensive harm that would occur if Plaintiffs' and class members' Private Information were exposed through a Data Breach, and thus owed a duty to safeguard that information. Given the sensitive nature of the Private Information, T-Mobile knew that hackers and cybercriminals would be able to commit identity theft, financial fraud, phishing, socially-engineered attacks, and other identity-related fraud if they were able to exfiltrate that data from T-Mobile's servers. T-Mobile also knew that individuals whose Private Information was stored on T-Mobile's servers would be reasonable in spending time and effort to mitigate any harm arising from a breach and prevent identity theft and fraud if that data were exfiltrated.

[7] https://www.reuters.com/technology/hackers-steal-some-personal-data-about-78-mln-t-mobile-customers-2021-08-18/

LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP

Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

26. Despite T-Mobile's representations that it cares about its customers and protects its customers' data, it has a deficient security program and no means to effectively manage or govern the data it holds, as this Data Breach and T-Mobile's prior data breaches illustrate. Here, the data stolen was unencrypted. T-Mobile knew this information was (a) unencrypted and thus subject to breach and misuse; (b) included highly sensitive PII; and (c) was not in transit and being actively used. The failure to encrypt this obsolete data containing highly sensitive PII was particularly flagrant and egregious. There was no valid reason for retaining this highly sensitive PII, including SSNs, and T-Mobile's lax treatment of this PII made public exposure through a cyberattack highly likely.

27. T-Mobile knew of the attendant risks that it and its customers faced as a result of hosting the Private Information of tens of millions of individuals. Furthermore, at all relevant times, T-Mobile knew the Private Information stored on its servers was valuable and at risk of cyberattack given the previous data breaches it suffered. The importance of developing a cybersecurity plan is more acute now than ever, as data breaches become more prevalent. Accordingly, T-Mobile was on notice of the harms that could ensue if it failed to protect individuals' Private Information.

C. T-Mobile Failure Resulted in the Data Breach

28. Before the Data Breach, Plaintiffs and class members provided sensitive and personally identifying Private Information to T-Mobile as part of signing up for a service plan with or financing a device through T-Mobile. When providing such information, Plaintiffs and class members reasonably expected that the manager and securer of their Private Information, T-Mobile, would maintain security against cybercriminals and cyberattacks.

29. T-Mobile maintained Plaintiffs' and the class members' data on servers with compromised security. Despite its own awareness of steady increases of cyberattacks on businesses in various industries over the course of recent years, T-Mobile did noy maintain adequate security over Plaintiffs' and the class members' Private Information and did not adequately protect it against hackers and cyberattacks.

LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP

Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

30. "T-Mobile has had 6 other data breaches in the past 4 years," said Doug Schmidt, a professor of computer science at Vanderbilt University. "It appears that their IT system is particularly vulnerable since they haven't been able to rectify their known security issues during this time period, which should be concerning to customers."[8]

31. T-Mobile has not been transparent about the six data breaches and how they occurred. T-Mobile's lack of transparency means that Plaintiffs and class members still do not know how T-Mobile restricted access to Private Information or the extent to which it practiced cybersecurity hygiene, such as data minimization or deleting data after a certain period of time. Similarly, T-Mobile has completely failed to provide basic information about the Data Breach itself to the public—including when it was actually first detected; which security and privacy practices were insufficient (or not followed) so as to allow the Data Breach to occur; what T-Mobile is doing to prevent future data breaches; and how class members might be affected if cybercriminals target the individuals whose Private Information was taken. T-Mobile's lack of clarity about the extent of the information that was comprised has left Plaintiffs and class members to fend for themselves, spending time, effort, and money to protect themselves in the wake of the Data Breach.

32. As a result of T-Mobile's lax data protection standards, cybercriminals obtained access not only to recently obtained information, but Private Information that remained on backup files from the mid-1990s. The Data Breach was the result of T-Mobile's failure not only to properly and adequately determine whether it was susceptible to a data breach but also its negligent and reckless failure to remove data containing Private Information or to encrypt such information. T-Mobile, in fact, had no valid business reason for retaining such records containing highly sensitive Private Information—including SSNs—for such long periods and for failing to delete or encrypt such information. The failure was knowing, reckless and, at bare minimum,

[8] https://www.reuters.com/technology/t-mobile-says-hackers-accessed-data-another-53-mln-subscribers-2021-08-20/

LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP

Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

negligent given the known risks to T-Mobile. The breach of Plaintiffs and class members' Private Information, particularly their SSNs, is a direct consequence of this conduct.

33. T-Mobile has obligations and duties created by state and federal law, contracts, industry standards, common law, and representations made to the clients who entrusted Plaintiffs' and others' data to T-Mobile's care to keep Private Information secure, confidential, and protected from unauthorized access and disclosure.

34. T-Mobile breached its obligations to Plaintiffs and the class members, and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard T-Mobile's computer systems and data. T-Mobile's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

(a) Failing to maintain an adequate data security program to reduce the risk of data breaches and cyberattacks;

(b) Failing to adequately protect consumers' Private Information;

(c) Failing to properly monitor its own data security programs for existing intrusions; and

(d) Failing to destroy highly confidential personal data information including Social Security numbers which was unnecessarily kept on T-Mobile's serves despite no reasonable or practicable business reason for doing so.

35. As the result of T-Mobile's failure to take certain measures to prevent the attack before it occurred, T-Mobile negligently and unlawfully failed to safeguard Plaintiffs' and class members' Private Information.

36. Accordingly, as outlined below, Plaintiffs' daily lives were disrupted; Plaintiffs and class members experienced actual incidents of identity theft and fraud, and Plaintiffs and class members face an increased risk of fraud and identity theft.

D. The Data Breach Harmed Customers and Putative Customers

37. Plaintiffs, class members, and putative T-Mobile customers suffered actual injury from having their Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of their Private Information, a form of

property that T-Mobile obtained from Plaintiffs, class members, and putative T-Mobile customers; (b) violation of their privacy rights; (c) imminent and impending injury arising from the increased risk of identity theft and fraud; (d) emotional distress; and (e) time and resources spent mitigating the harm.

38. Plaintiff Lam has suffered emotional distress as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Indeed, Plaintiff Lam discovered that she was the subject of identity theft after T-Mobile confirmed the Data Breach. Plaintiff Lam is very concerned about further identity theft and fraud as well as the consequences of such identity theft and fraud resulting from the Data Breach. As a result of the Data Breach, she feels that she will continue to be at increased risk of identity theft and fraud for years to come.

39. Plaintiff Phan feels her privacy has been invaded. She anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, she feels that she will continue to be at increased risk of identity theft and fraud for years to come.

40. Private Information is valuable property. Its value is axiomatic, considering the market value and profitability of "Big Data" corporations in America. Illustratively, Alphabet Inc., the parent company of Google, reported in its 2020 Annual Report a total annual revenue of $182.5 billion and net income of $40.2 billion. $160.7 billion of this revenue is derived from its Google business, which is driven almost exclusively by leveraging the Private Information it collects about users of its various free products and services. America's largest corporations profit almost exclusively through the use of Private Information, illustrating the considerable market value of personal Private Information.

41. Criminal law also recognizes the value of Private Information and the serious nature of the theft of such an asset by imposing prison sentences. This strong deterrence is necessary because cybercriminals earn significant revenue through stealing Private Information. Once a cybercriminal has unlawfully acquired personal data, the criminal can demand a ransom or

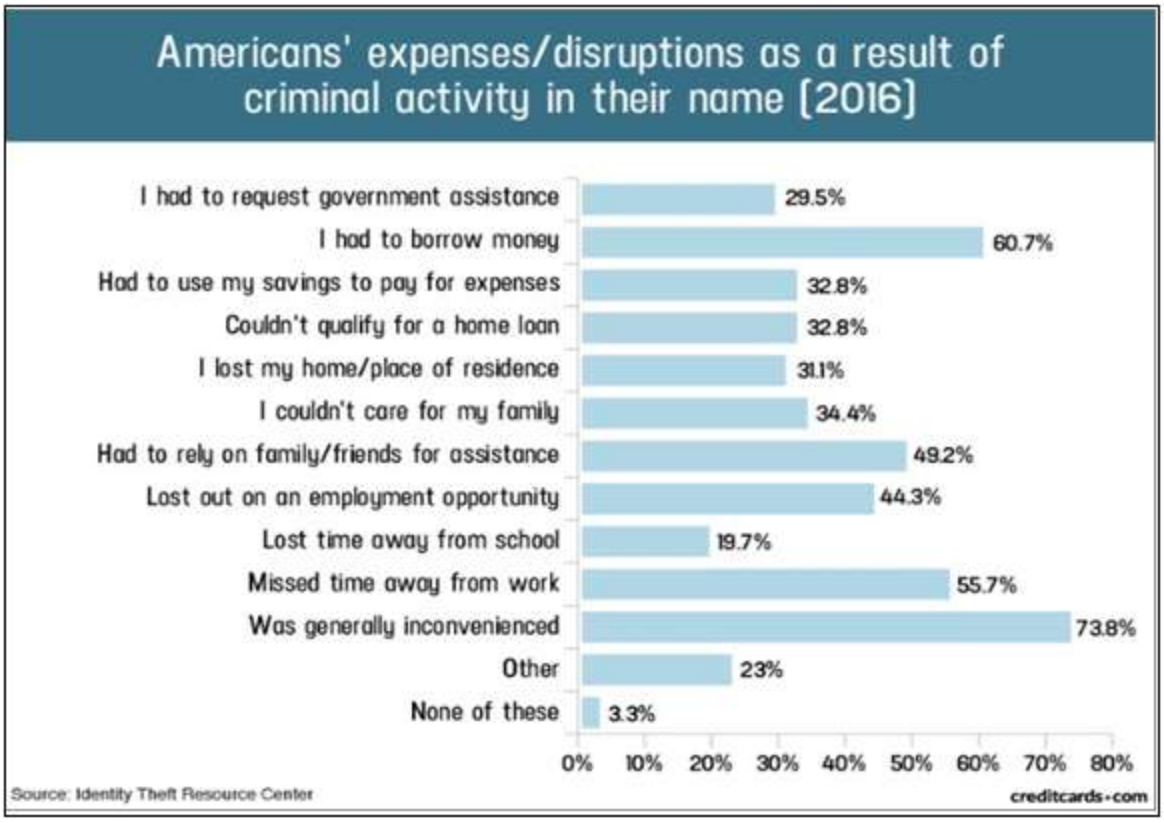
blackmail payment for its destruction, use the information to commit fraud or identity theft, or sell the Private Information to another cybercriminal on a thriving black market.

42. Once stolen, Private Information can be used in a number of different ways. One of the most common is that it is offered for sale on the "dark web," a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and Private Information. Websites appear and disappear quickly, making it a dynamic environment.

43. Cybercriminals use stolen Private Information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. Identity thieves can also use SSNs, which are immutable, to obtain a driver's license or other official identification card in the victim's name, but with the thief's picture; use the victim's name and SSN to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house or receive medical services in the victim's name, seek unemployment or other benefits, and may even give the victim's Private Information to police during an arrest resulting in an arrest warrant being issued in the victim's name. A study by the Identity Theft Resource Center ("ITRC") shows the multitude of harms caused by fraudulent use of personal and financial information:

/ / /

/ / /



44. As set forth above, 96.7% of study subjects experienced costs or other harms from the criminal activity. As illustrated in the above graphic, this includes devastating results such as "I lost my home/place of residence" and "I couldn't care for my family." Private Information is a valuable property right.[9] Its value is axiomatic, considering the value of Big Data in corporate America as well as the consequences of cyber thefts resulting in heavy prison sentences. This obvious risk to reward analysis illustrates that Private Information has considerable market value that is diminished when it is compromised.

45. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the GAO, which conducted a study regarding data breaches:

[9] *See, e.g.*, John T. Soma et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *1 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.").

LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP
Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[10]

46. Private Information is such an inherently valuable commodity to identity thieves that, once it compromised, criminals often trade the information on the cyber black-market for years.

47. Furthermore, data breaches that expose any personal data, and in particular non-public data of any kind, directly and materially increasethe chance that a potential victim is targeted by a spear phishing attack in the future, and spear phishing results in a high rate of identity theft, fraud, and extortion.[139]

48. There is a strong probability that entire batches of stolen information from the Data Breach have yet to be made available on the black market, meaning Plaintiffs and the class members are at an increased risk of fraud and identity theft for many years into the future. Indeed, some of the Plaintiffs and many of the Class Members are in very early stages of their lives—in their twenties and thirties—when they first sign up for a service plan with T-Mobile or finance a device through T-Mobile. Thus, Plaintiffs must vigilantly monitor their financial accounts for many years to come.

V. PLAINTIFFS' AND CLASS MEMBERS' INJURIES AND DAMAGES

49. Plaintiffs and class members have been harmed and incurred damages as a result of the compromise of their Private Information in the Data Breach. Plaintiffs' Private Information was compromised as a direct and proximate result of the Data Breach.

50. Plaintiffs have lost the value of their Private Information because the information is a valuable commodity. The cybercriminals also recognize its value by advertising it for sale on the black web.

[10] GAO Report, *supra* n.131, at 29.

LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP

Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

51. Plaintiffs and class members face immediate and substantial risk of identity theft or fraud, such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

52. Plaintiffs and the class members also face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs.

53. Plaintiffs and the class members have suffered or will suffer actual injury as a direct result of the Data Breach. Plaintiffs and the class members have and will suffer ascertainable losses in the form of out-of-pocket expenses and/or the loss of the value of their time spent in reasonably acting to remedy or mitigate the effects of the Data Breach relating to:

(a) Finding fraudulent charges;

(b) Canceling and reissuing credit and debit cards;

(c) Addressing their inability to withdraw funds linked to compromised accounts;

(d) Taking trips to banks and waiting in line to obtain funds held in limited accounts;

(e) Placing "freezes" and "alerts" with credit reporting agencies;

(f) Spending time on the phone with or at a financial institution to dispute fraudulent charges;

(g) Contacting financial institutions and closing or modifying financial accounts;

(h) Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

(i) Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled;

(j) Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come; and

(k) Interacting with government agencies and law enforcement to address the impact and harm caused by this breach.

54. As a result of the Data Breach, Plaintiff and class members suffered actual injury from having their Private Information compromised as a result of the Data Breach including, but not limited to, (a) damage to and diminution in the value of their Private Information, a form of property that T-Mobile obtained from Plaintiffs; (b) violation of their privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

55. As a result of the Data Breach, Plaintiff and class members tried to mitigate its impact after learning about it in the news, including by reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud and by monitoring online banking to resolve issues related to the Data Breach. This time spent reviewing credit monitoring reports and/or banking account statements for irregularities is valuable time Plaintiffs otherwise would have spent on other activities, including, but not limited to work and/or recreation. Plaintiffs and class members will have to continue to spend significant amounts of time to respond to the Data Breach and monitor their financials and records for misuse.

56. As a result of the Data Breach, Plaintiff and class members have suffered emotional distress as a result of the release of their Private Information, which they believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using their Private Information for purposes of identity theft and fraud. Plaintiffs are very concerned about identity theft and fraud as well as the consequences of such identity theft and fraud resulting from the Data Breach. Plaintiffs reasonably believe that their Private Information is available for purchase on the dark web and that they will experience actual identity thief or fraud.

57. Finally, Plaintiffs and class members, at the very least, sustained nominal damages for T-Mobile's violations as discussed herein. As a result of T-Mobile's failures to safeguard Plaintiffs' and the class members' Private Information, they are forced to live with the knowledge that their Private Information—which contains private and personal details of their life—may be disclosed to the entire world, thereby making them vulnerable to cybercriminals, permanently

subjecting them to loss of security, and depriving Plaintiffs and the class members of their fundamental right to privacy.

58. Plaintiffs are entitled to statutory damages, as provided, based upon the relevant causes of action alleged herein, and described below. Plaintiffs and the class members have an interest in ensuring that their Private Information, which remains in the possession of T-Mobile, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing Plaintiffs' and the class members' data is limited and secured.

VI. CLASS ACTION ALLEGATIONS

59. Plaintiffs bring this action on their own behalf and on behalf of all natural persons similarly situated, as referred to throughout this Complaint as "class members."

60. Pursuant to Federal Rules of Civil Procedure 23(b)(2) and (b)(3), and (c)(4) as applicable, Plaintiffs propose the following class definitions, subject toamendment as appropriate:

> **Nationwide Class:** All natural persons residing in the United States whose Personally Identifiable Information was compromised as a result of the T-Mobile Data Breach.
>
> **California Subclass:** All natural persons residing in California whose Personally Identifiable Information was compromised as a result of the T-Mobile Data Breach.
>
> **Hawaii Subclass:** All natural persons residing in Hawaii whose Personally Identifiable Information was compromised as a result of the T-Mobile Data Breach.
>
> **Washington Subclass:** All natural persons residing in Washington whose Personally Identifiable Information was compromised as a result of the T-Mobile Data Breach.

61. Excluded from the Class and Subclasses are T-Mobile's officers, directors, and employees; any entity in which T-Mobile has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of T-Mobile. Excluded also from the Class and Subclasses are members of the judiciary to whom this case is assigned, their families, and members of their staff.

62. **Numerosity under Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous and geographically dispersed that individual joinder of all class members is impracticable. While the exact number of class members is unknown to Plaintiffs at

this time, based on information and belief, the class consists of at least 48 million persons whose data was compromised in the Data Breach, who can be identified by reviewing the Private Information exfiltrated from T-Mobile's databases.

63. **Commonality under Federal Rule of Civil Procedure 23(a)(2).** There are questions of law and fact common to Plaintiffs and class members, which predominate over any questions affecting only individual class members. These common questions of law and fact include, without limitation:

(a) Whether T-Mobile unlawfully used, maintained, lost, or disclosed Plaintiffs' and the class members' Private Information;

(b) Whether T-Mobile failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

(c) Whether T-Mobile truthfully represented the nature of its security systems, including their vulnerability to hackers;

(d) Whether T-Mobile's data security programs before and during the Data Breach complied with applicable data security laws;

(e) Whether T-Mobile's data security programs before and during the Data Breach were consistent with industry standards;

(f) Whether T-Mobile owed a duty to class members to safeguard their Private Information;

(g) Whether T-Mobile breached its duty to class members to safeguard their Private Information;

(h) Whether cyberhackers obtained, sold, copied, stored or released class members' Private Information;

(i) Whether T-Mobile knew or should have known that its data security programs and monitoring processes were deficient;

(j) Whether the class members suffered legally cognizable damages as a result of T-Mobile's misconduct;

(k) Whether T-Mobile's conduct was negligent;

(l) Whether T-Mobile's conduct was negligent *per se*;

(m) Whether T-Mobile's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

(n) Whether T-Mobile failed to provide accurate and complete notice of the Data Breach in a timely manner; and

(o) Whether the class members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

64. **Typicality under Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of those of the class members because Plaintiffs' Private Information, like that of every class member, was compromised in the Data Breach.

65. **Adequacy of Representation under Federal Rule of Civil Procedure (a)(4).** Plaintiffs will fairly and adequately represent and protect the interests of class members, including those from states and jurisdictions where they do not reside. Plaintiffs' Counsel are competent and experienced in litigating class actions and were appointed to lead this litigation by the Court pursuant to Federal Rule of Civil Procedure 23(g).

66. **Predominance under Federal Rule of Civil Procedure 23(b)(3).** T-Mobile has engaged in a common course of conduct toward Plaintiffs and the class members, in that all Plaintiffs' and the class members' data at issue here was stored by T-Mobile and accessed during the Data Breach. The common issues arising from T-Mobile's conduct affecting class members, as described *supra*, predominate over any individualized issues. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

67. **Superiority under Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most class members would find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy.

LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP

Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

68. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for T-Mobile. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

69. **Injunctive Relief is Appropriate under Federal Rule of Civil Procedure 23(b)(2).** T-Mobile has failed to take actions to safeguard Plaintiffs' and class members' Private Information such that injunctive relief is appropriate and necessary. T-Mobile has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a classwide basis.

70. **Issue Certification Appropriate under Federal Rule of Civil Procedure 23(c)(4).** In the alternative, this litigation can be brought and maintained a class action with respect to particular issues, such as T-Mobile's liability with respect to the foregoing causes of action.

VII. CAUSES OF ACTION

71. Plaintiffs bring these causes of action on behalf of the Nationwide Class. The application of one specific state's laws to any cause of action is premature at this juncture, without the benefit of discovery.

72. Based on information and belief, individuals from all states and the District of Columbia suffered injuries as a direct and proximate result of the Data Breach. Plaintiffs have standing to represent individuals in every jurisdiction. To force Plaintiff to search for specific, named representatives for all states at this stage in the litigation serves no useful purpose. *See*, *e.g.*, *In re Equifax, Inc., Customer Data Security Breach Litig.*, 362 F. Supp. 3d 1295, 1344 (N.D. Ga. 2019); *In re Target Corp. Data Security Breach Litig.*, 66 F. Supp. 3d 1154, 1160 (D. Minn. 2014).

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS
OR ALTERNATIVELY, ON BEHALF OF PLAINTIFFS AND THE SUBCLASSES

COUNT 1: NEGLIGENCE

73. Plaintiffs repeat and reallege all preceding paragraphs, as if fully alleged herein.

74. T-Mobile required Plaintiffs and class members to submit non-public, personal information to obtain plans and/or devices from T-Mobile.

75. In providing their Private Information, Plaintiffs and class members had a reasonable expectation that this information would be securely maintained and not easily accessible to, or exfiltrated by cybercriminals.

76. Further, Plaintiffs and class members had a reasonable expectation that in the event of a Data Breach, T-Mobile would provide timely and adequate notice to them and would properly identify what Private Information was exposed during a Data Breach so that Plaintiffs and class members could take prompt and appropriate steps to safeguard their identities.

77. T-Mobile, as an entity that collects sensitive, private data from consumers, such as Plaintiffs and class members, and likewise stores and maintains that data, has both a contractual duty and a duty arising independently from any contract to protect that information.

78. Specifically, T-Mobile, as the purported expert guardian and gatekeeper of data, had a duty to Plaintiffs and class members to securely maintain the Private Information collected as promised, warranted, and in a reasonable manner which would prevent cybercriminals from accessing and exfiltrating this information.

79. By undertaking the duty to maintain and secure this data, sharing it and using it for commercial gain, T-Mobile had a duty of care to use reasonable means to secure and safeguard its systems and networks—and Plaintiffs and class members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from cyber theft.

80. T-Mobile's duty included a responsibility to implement systems and processes by which it could detect and prevent a breach of its security systems in an expeditious manner and to give prompt and adequate notice to those affected by a data breach.

81. T-Mobile owed a duty of care to Plaintiffs and class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected and safeguarded the Private Information of the Plaintiffs and the Class.

LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP

Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

82. T-Mobile's duty of care to use reasonable security measures arose as a result of the special relationship that existed between T-Mobile and Plaintiffs and class members. It is recognized by T-Mobile's Privacy Policy as well as applicable laws. Specifically, T-Mobile actively solicited Private Information as part of its business and was solely responsible for and in the position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and class members from a resulting Data Breach.

83. Likewise, as the guardian and gatekeeper of Plaintiffs and class members' Private Information, a special duty existed between T-Mobile and Plaintiffs and class members, one that required T-Mobile to promptly and adequately provide notice of the Data Breach in a manner that would allow Plaintiffs and class members to take prompt and appropriate steps to safeguard their identities.

84. T-Mobile also had a common law duty to prevent foreseeable harm to others. Plaintiffs and class members were the foreseeable and probable victims of any inadequate security practices. It was foreseeable that Plaintiffs and class members would be harmed by the failure to protect their personal information because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

85. T-Mobile knew or should have known that the Plaintiffs and class members were relying on T-Mobile to adequately safeguard and maintain their Private Information.

86. Based on T-Mobile's history of Data Breaches, T-Mobile management was on notice that T-Mobile's systems and networks at issue in this Data Breach were vulnerable, not secure, and that a cybercriminal attack may be successful. Nevertheless, T-Mobile ignored the warnings and failed to improve its data safeguards and secure Plaintiffs and class members' Private Information.

87. T-Mobile had additional duties to safeguard Plaintiffs and class members' data pursuant to the FTC Act, 15 U.S.C. § 45. Under this statute, T-Mobile had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and class members' Private Information.

88. T-Mobile's duty to use reasonable care in protecting confidential data also because T-Mobile is bound by industry standards to protect confidential Private Information.

89. T-Mobile breached its duties, and thus was negligent, by failing to use reasonable measures to protect the Plaintiffs and class members' data. The specific negligent acts and omissions committed by T-Mobile include, but are not limited to, the following:

(a) Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs and class members' Private Information;

(b) Failing to adequately monitor the security of its networks and systems;

(c) Failure to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

(d) Allowing unauthorized access to and exfiltration of Plaintiffs and class members' Private Information;

(e) Failing to timely detect that Plaintiffs and class members' Private Information had been compromised;

(f) Failing to provide timely notice that Plaintiffs and class members' Private Information had been compromised so those at risk could take timely and appropriate steps to mitigate the potential for identity theft and other damages; and

(g) Failing to provide adequate notice of what Private Information had been compromised so that Plaintiffs and class members at risk could take timely and appropriate steps to mitigate the potential for identify theft and other damages.

90. It was foreseeable to T-Mobile that its failure to use reasonable measures to protect Plaintiffs and the class members' Private Information, including when it warned its systems and networks were vulnerable to cyberattack, would result in injury to Plaintiffs and class members. Further, the breach of security was reasonably foreseeable given the known high frequency of Data Breaches.

91. It was additionally foreseeable to T-Mobile that failure to timely and adequately provide notice of the Data Breach would result in Plaintiffs and class members not being afforded the ability to timely safeguard their identities.

92. It was therefore foreseeable to T-Mobile that its failure to adequately safeguard Plaintiffs and class members' Private Information or provide timely and adequate notice of the Data Breach, would result in one or more types of injuries to Plaintiffs and the class members.

93. Plaintiffs are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

94. Plaintiffs are also entitled to injunctive relief requiring T-Mobile to, *e.g.*, (i) strengthen its data security programs and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide robust and adequate credit monitoring to all class members, and any other relief this Court deems just and proper.

COUNT 2: NEGLIGENCE *PER SE*

95. Plaintiffs repeat and reallege all preceding paragraphs, as if fully alleged herein.

96. T-Mobile had a legal duty to safeguard Plaintiffs and class members' data.

97. Pursuant to the FTC Act, 15 U.S.C. § 45, T-Mobile had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and class members' Private Information. Similar state-specific statutory causes of action—such as consumer fraud and unfair trade practices acts—provide for such a duty, as well.

98. Plaintiffs and class members are members of the classes of persons the foregoing statute is intended to protect.

99. The essential purposes of these statutes are to protect from the same or similar kind of harm caused to Plaintiffs and class members, as a direct and proximate result of T-Mobile's breach of those statutory and regulatory duties.

100. T-Mobile breached its duties to Plaintiffs and class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs and class members' Private Information.

101. T-Mobile's breach of its duties arising out of the foregoing statute constitutes negligence per se.

102. But for T-Mobile's wrongful and negligent breach of its duties owed to Plaintiffs and class members, Plaintiffs and class members' data would not have been compromised and they would not have been harmed.

103. The injury and harm suffered by Plaintiffs and class members was the reasonably foreseeable result of T-Mobile's breach of its duties. T-Mobile knew or should have known that it was failing to meet its duties, and that T-Mobile's breach would cause Plaintiffs and class members to experience the foreseeable harms associated with the exposure of their Private Information, including increased risk of identity theft.

104. As a direct and proximate result of T-Mobile's violation of the foregoing statute, Plaintiffs and class members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT 3: GROSS NEGLIGENCE

105. Plaintiffs repeat and reallege all preceding paragraphs, as if fully alleged herein.

106. Plaintiffs were required to submit non-public Private Information to purchase a plan and/or device from T-Mobile. T-Mobile had a duty to Plaintiffs to securely maintain the Private Information collected as promised and warranted.

107. T-Mobile maintained unencrypted Private Information, however, on certain servers.

108. T-Mobile knew this information was (a) unencrypted and thus subject to breach and misuse; (b) included highly sensitive Private Information; and (c) was not in transit and being actively used.

109. The failure to encrypt this obsolete data containing highly sensitive Private Information on legacy and/or back-up versions of T-Mobile servers was particularly flagrant and egregious. Indeed, this unencrypted Private Information made public exposure of this Private Information in a cyberattack very likely.

110. Moreover, there was no reasonable reason for retaining these records which contain highly sensitive Private Information, including date of birth, social security number, and driver's

license/ID information. As a result of T-Mobile's conduct, Plaintiffs' highly sensitive, unencrypted Private Information was accessed, exfiltrated and otherwise exposed by the Data Breach

111. By voluntarily accepting the duty to maintain and secure this data, and sharing it and using it for commercial gain, T-Mobile had a duty of care to use reasonable means to secure and safeguard its computer systems to prevent disclosure of the information, and to safeguard the information from cyber theft.

112. T-Mobile's duty included a responsibility to implement systems and processes by which it could detect and prevent a breach of its security systems in an expeditious manner and to give prompt notice to those affected by a Data Breach.

113. T-Mobile owed a duty of care to Plaintiffs to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected and safeguarded Plaintiffs' Private Information.

114. T-Mobile owed an additional duty to Plaintiffs to take measures to ensure that, *inter alia*:

(a) all Private Information was encrypted and continued to be encrypted;

(b) Private Information is deleted after a reasonable amount of time; and/or

(c) Plaintiffs were notified that their sensitive and unencrypted Private Information had continued to be stored.

115. T-Mobile's duty of care to use reasonable security measures arose as a result of the special relationship that existed between T-Mobile and Plaintiffs, which is recognized by T-Mobile's Privacy Policy as well as applicable laws. T-Mobile actively solicited Private Information as part of its business and was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs from the Data Breach.

116. Pursuant to the FTC Act, 15 U.S.C. § 45, T-Mobile had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and the class members' Private Information. Plaintiffs and the class members are the individuals whom the FTC Act is intended to protect.

LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP

Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

117. T-Mobile's duty to use reasonable care in protecting confidential data arose not only as a result of the statute and described above but also because T-Mobile is bound by industry standards to protect confidential Private Information.

118. T-Mobile consciously failed to use reasonable measures to protect Plaintiffs and class members' data. The specific gross negligent acts and omissions committed by T-Mobile include, but are not limited to, the following:

(a) Consciously ailing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs and class members' Private Information;

(b) Consciously failing to ensure all sensitive Personal Information was encrypted;

(c) Consciously failing to ensure all obsolete data was destroyed in a reasonable amount of time;

(d) Consciously failing to notify Plaintiffs and class members that their unencrypted data was still maintained by T-Mobile;

(e) Consciously failing to adequately monitor the security of its networks and systems;

(f) Consciously failing to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

(g) Consciously allowing unauthorized access to class members' Private Information;

(h) Consciously failing to detect in a timely manner that class members' Private Information had been compromised; and

(i) Consciously failing to timely notify Plaintiffs and class members about the Data Breach so those put at risk could take timely and appropriate steps to mitigate the potential for identity theft and other damages.

119. It was foreseeable that T-Mobile's conscious failure to use reasonable measures to protect the Plaintiffs class members' Private Information would result in injury to the Plaintiffs and

class members. Further, the breach of security was reasonably foreseeable given the known high frequency of Data Breaches.

120. It was therefore foreseeable that the conscious failure to adequately safeguard Plaintiffs and class members' Private Information would result in one or more types of injuries to Plaintiffs and class members.

121. Plaintiffs and class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

122. Plaintiffs and class members are also entitled to injunctive relief requiring T-Mobile to, *e.g.*, (i) identify all backup data it still maintains; (ii) destroy or encrypt backup data that has been obsolete for an unreasonable amount of time; (iii) notify all consumers with backup data that is still be maintained by T-Mobile; (iv) strengthen its data security programs and monitoring procedures; (v) submit to future annual audits of those systems and monitoring procedures; and (vi) immediately provide robust and adequate credit monitoring to Plaintiffs and class members, and any other relief this Court deems just and proper.

COUNT 4: INVASION OF PRIVACY

123. Plaintiffs repeat and reallege all preceding paragraphs, as if fully alleged herein.

124. Plaintiffs and class members have a legally protected privacy interest in their Private Information, which is and was collected, stored and maintained by T-Mobile, and they are entitled to the reasonable and adequate protection of their Private Information against foreseeable unauthorized access, as occurred with the Data Breach.

125. Plaintiffs and class members reasonably expected that T-Mobile would protect and secure their Private Information from unauthorized parties and that their Private Information would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

126. T-Mobile unlawfully invaded the privacy rights of Plaintiffs and the class members by engaging in the conduct described above, including by failing to protect their Private Information by permitting unauthorized third parties to access, exfiltrate, and view this Private Information.

127. This invasion of privacy resulted from T-Mobile's failure to properly secure and maintain Plaintiffs, the Class and Subclasses members' Private Information, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

128. Plaintiffs, the Class and Subclasses members' Private Information is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiffs class members' Private Information, and such Information is otherwise protected from exposure to the public by law.

129. The disclosure of Plaintiffs, the Class and Subclasses members' Private Information to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

130. T-Mobile's willful and reckless conduct which permitted unauthorized access, exfiltration, and disclosure of Plaintiffs' and the Class and Subclasses members' sensitive, Private Information is such that it would cause serious mental injury to people of ordinary sensibilities.

131. The unauthorized access, exfiltration, and disclosure of Plaintiffs, the Class and Subclasses members' Private Information was without their consent and in violation of the law.

132. As a result of the invasion of privacy caused by T-Mobile, Plaintiffs and class members suffered and will continue to suffer damages and injury as set forth herein.

133. Plaintiffs, the class members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, reasonable attorneys' fees and costs, and any other relief that is just and proper.

COUNT 5: BREACH OF IMPLIED CONTRACT

134. Plaintiffs repeat and reallege all preceding paragraphs, as if fully alleged herein.

135. T-Mobile provided plans and/or devices to Plaintiffs and class members. In exchange, T-Mobile received benefits in the form of monetary payments and/or other valuable consideration (*e.g.*, access to their private and personal data).

136. T-Mobile has acknowledged these benefits and accepted or retained them.

LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP

Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

137. In signing up for T-Mobile's plans and/or purchasing devices through T-Mobile, Plaintiffs and class members provided T-Mobile with their private and personal information.

138. By providing that information, and upon T-Mobile's acceptance of that information, Plaintiffs and class members, on the one hand, and T-Mobile, on the other, entered into implied contracts whereby T-Mobile agreed to and was obligated to take reasonable steps to secure and safeguard that Private Information. Such safeguarding was integral and essential to T-Mobile's business of providing data services and devices.

139. Under those implied contracts, T-Mobile was obligated to provide Plaintiffs and class members with plans and/or devices and safeguard their Private Information Instead, T-Mobile was incapable of providing safety and security and made such Private Information vulnerable to unauthorized access.

140. Without such implied contracts, Plaintiffs and class members would not have signed up for a plan and/or purchased a device through T-Mobile and would not have conferred benefits on T-Mobile, but rather chosen alternative data and device services that did not present these privacy and safety risks.

141. Plaintiffs and Class members fully performed their obligations under these implied contracts.

142. As described throughout, T-Mobile did not take reasonable steps to safeguard Plaintiffs' and Class members' private information. In fact, Defendant willfully violated those privacy interests by maintaining lax data security on its servers.

143. Because T-Mobile failed to take reasonable steps to safeguard Plaintiffs' Private Information, T-Mobile breached its implied contracts with Plaintiffs and Class members.

144. T-Mobile's failure to fulfill its obligation to safeguard Plaintiffs' and Class members' private information resulted in the security breach.

145. Stated otherwise, because Plaintiffs and Class members provided valuable consideration for privacy protections they did not receive—even though such protections were a material part, if not the very essence, of their contracts with Defendant—the full benefit of their bargain.

LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP

Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

146. As a result of T-Mobile's conduct, Plaintiffs and members of the Class have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

147. Accordingly, Plaintiffs, on behalf of themselves and class members, seeks an order declaring that T-Mobile's conduct constitutes breach of implied contract, and awarding them damages in an amount to be determined at trial.

COUNT 6: BREACH OF IMPLIED COVENANT

OF GOOD FAITH AND FAIR DEALING

148. Plaintiffs repeat and reallege all preceding paragraphs, as if fully alleged herein.

149. There is a covenant of good faith and fair dealing implied in every implied contract. This implied covenant requires each contracting party to refrain from doing anything to injure the right of the other to receive the benefits of the agreement. To fulfill its covenant, a party must give at least as much consideration to the interests of the other party as it gives to its own interests.

150. Under the implied covenant of good faith and fair dealing, T-Mobile is obligated to, at a minimum, (a) implement proper procedures to safeguard the personal information of Plaintiffs and other class members; (b) refrain from disclosing, without authorization or consent, the personal information of Plaintiffs and other class members to any third parties; (c) promptly and accurately notify Plaintiffs and other class members of any unauthorized disclosure of, access to, and use of their personal information; and (d) maintain adequate security and proper encryption in T-Mobile's severs.

151. T-Mobile breached the implied covenant of good faith and fair dealing by, among other things:

(a) Failing to maintain adequate security and proper encryption on T-Mobile's servers;

(b) Allowing third parties to access the Private Information of Plaintiffs and class members;

(c) Failing to implement and maintain adequate security measures to safeguard Plaintiffs and class members' personal information; and

(d) failing to timely notify Plaintiffs and other Class members of the unlawful disclosure of their Private Information.

152. As a direct and proximate result of T-Mobile's breaches of the implied covenant of good faith and fair dealing, Plaintiffs and other Class members have suffered actual losses and damages.

COUNT 7: UNJUST ENRICHMENT

153. Plaintiffs repeat and reallege all preceding paragraphs, as if fully alleged herein.

154. Plaintiffs, the Class and Subclass members have an interest, both equitable and legal, in the Private Information about them that was collected, secured, and maintained by T-Mobile and that was ultimately compromised in the Data Breach.

155. A financial benefit was conferred upon T-Mobile when Plaintiffs, the Class and Subclass members provided their Private Information to T-Mobile in conjunction with signing up for a plan with, or purchasing a device through, T-Mobile. T-Mobile's business model would not exist save for the need to ensure the security of Plaintiffs' and class members' Private Information.

156. The relationship between T-Mobile and Plaintiffs, the Class and Subclass members is not attenuated, as Plaintiffs, the Class and Subclass members had a reasonable expectation that the security of their information would be maintained when they provided their information to T-Mobile. Plaintiffs, the Class and Subclass members were induced to provide their information in reliance on the fact that T-Mobile's stated data security measures were adequate.

157. On information and belief, this financial benefit was, in part, conferred when portions of Plaintiffs, Class, and Subclass members' payments were used by T-Mobile for maintenance of its servers.

158. T-Mobile realized the benefit of such payments in connection with the maintenance of its servers. T-Mobile also understood and appreciated that the Private Information pertaining to Plaintiffs, the Class and Subclasses members was private and confidential and its value depended upon T-Mobile maintaining the privacy and confidentiality of that Private Information.

159. But for T-Mobile's willingness and commitment to properly and safely collect, maintain and secure the Private Information would not have been transferred to and entrusted with T-Mobile. Further, if T-Mobile had disclosed that its data security measures were inadequate, T-Mobile would not have gained the trust of its customers.

160. As a result of T-Mobile's wrongful conduct as alleged in this Complaint (including among things its utter failure to employ adequate data security measures, its continued maintenance and use of the Private Information belonging to Plaintiffs, the Class and Subclass members without having adequate data security measures, and its other conduct facilitating the theft of that Private Information), T-Mobile has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs, the Class and Subclasses members. Among other things, T-Mobile continues to benefit and profit from using that Private Information while its value to Plaintiffs and Class and Subclasses members has been diminished.

161. T-Mobile's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the collection, maintenance, and inadequate security of Plaintiffs, the Class and Subclasses members' sensitive Private Information, while at the same time failing to maintain that information secure from unauthorized access and exfiltration by cyber criminals.

162. It would be unjust, inequitable, and unconscionable for T-Mobile to be permitted to retain the benefits it received, and is still receiving, from Plaintiffs, the Class and Subclasses members in connection with the collection, maintenance and security of their Private Information. T-Mobile's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

163. The benefit conferred upon, received, and enjoyed by T-Mobile was not conferred officiously or gratuitously, and it would be inequitable and unjust for T-Mobile to retain the benefit.

164. T-Mobile is therefore liable to Plaintiffs, the Class, and Subclasses members for restitution in the amount of the benefit conferred on T-Mobile as a result of its wrongful conduct,

LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP

Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

including specifically the value to T-Mobile of the Private Information that was stolen in the Data Breach and the profits T-Mobile is receiving from the use of that information.

COUNT 8: DECLARATORY AND INJUNCTIVE RELIEF

165. Plaintiffs repeat and allege all preceding paragraphs, as if fully alleged herein.

166. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

167. An actual controversy has arisen in the wake of the Data Breach regarding its present and prospective common law and other duties to reasonably safeguard Plaintiffs and class members' Private Information and whether T-Mobile is currently maintaining data security measures adequate to protect Plaintiffs and class members from further, future Data Breaches that compromise their Private Information.

168. Plaintiffs and class members allege that T-Mobile's data security measures remain inadequate and T-Mobile has not provided any evidence that it has remedied the failure that occurred in the Data Breach at issue or has remedied any other vulnerability from its failure to properly assess threats by cybercriminals.

169. Plaintiffs and class members continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

170. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, *inter alia*, the following:

(a) T-Mobile continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a Data Breach under the common law and the FTC Act;

(b) T-Mobile owes a duty by virtue of its special relationship, understanding that it is safeguarding sensitive, Private Information, or that it has already

acknowledged a responsibility to keep such information safe by virtue of security policies; and

(c) T-Mobile continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

171. The Court also should issue corresponding prospective injunctive relief requiring T-Mobile to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information.

172. If an injunction is not issued, Plaintiffs and class members will suffer irreparable injury and lack an adequate legal remedy in the event of another Data Breach at T-Mobile. The risk of another such breach is real, immediate, and substantial. If another breach at T-Mobile occurs, Plaintiffs and class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

173. The hardship to Plaintiffs and class members if an injunction does not issue exceeds the hardship to T-Mobile if an injunction is issued. Among other things, if another massive Data Breach occurs at T-Mobile, Plaintiffs and class members will likely be subjected to substantial identify theft and other damage (as they cannot elect to store their information with another company). On the other hand, the cost to T-Mobile of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and T-Mobile has a pre-existing legal obligation to employ such measures.

174. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by helping to prevent another Data Breach at T-Mobile, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose Private Information would be further compromised.

/ / /

/ / /

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT 9: CALIFORNIA UNFAIR COMPETITION LAW,

Cal. Bus. & Prof. Code §§ 17200, *et seq.*

175. The California Plaintiff identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges all preceding paragraphs, as if fully alleged herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding unfair competition.

176. T-Mobile is a "person" as defined by Cal. Bus. & Prof. Code §17201.

177. T-Mobile violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

178. T-Mobile's "unfair" and "deceptive" acts and practices include:

(a) T-Mobile failed to implement and maintain reasonable security measures to protect Plaintiff and California Subclass members' Private Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. T-Mobile failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and the California Subclass, whose Private Information has been compromised.

(b) T-Mobile's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.*

(c) T-Mobile's failure to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not

outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of T-Mobile's inadequate security, consumers could not have reasonably avoided the harms that T-Mobile caused.

(d) Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

179. T-Mobile has engaged in "unlawful" business practices by violating multiple laws, including the FTC Act, 15 U.S.C. § 45.

180. T-Mobile's unlawful practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and California Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.*, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and California Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and 15 U.S.C. § 6801, *et seq.*;

(f) Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

(g) Failing to timely and adequately notify Plaintiff and California Subclass members of the Data Breach;

(h) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and California Subclass members' Private Information; and

(i) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by FTC Act, 15 U.S.C. § 45, and 15 U.S.C. § 6801, *et seq.*

181. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' Private Information.

182. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the California Subclass members, into believing that their Private Information was not exposed and misled Plaintiffs and the California Subclass members into believing they did not need to take actions to secure their identities.

183. As a direct and proximate result of T-Mobile's unfair, unlawful, and fraudulent acts and practices, Plaintiffs and California Subclass members were injured and lost money or property, including monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Private Information, including but not limited to the diminishment of their present and future property interest in their Private Information and the deprivation of the exclusive use of their Private Information.

184. T-Mobile acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs and California Subclass members' rights.

185. Plaintiffs and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from T-Mobile's unfair, unlawful, and fraudulent business practices or use of their Private Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT 10: CALIFORNIA CONSUMER LEGAL REMEDIES ACT,

Cal. Civ. Code §§ 1750, *et seq.*

186. The California Plaintiff identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges all preceding paragraphs, as if fully alleged herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer legal remedies.

187. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

188. T-Mobile is a "person" as defined by Civil Code §§ 1761(c) and 1770, and has provided "services" as defined by Civil Code §§ 1761(b) and 1770. Specifically, T-Mobile provides data plans and devices to customers.

189. As part of the services T-Mobile offers, T-Mobile touts its ongoing efforts to keep consumers' Private Information secure, including by ensuring ongoing compliance with legal privacy standards established both domestically and abroad, as recognized by T-Mobile's privacy policy.

LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP

Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

190. Plaintiffs and the California Class are "consumers" as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

191. T-Mobile's acts and practices were intended to and did result in the sales of products and services to Plaintiff and the California Subclass members in violation of Civil Code § 1770, including:

(a) Representing that goods or services have characteristics that they do not have;

(b) Representing that goods or services are of a particular standard, quality, or grade when they were not;

(c) Advertising goods or services with intent not to sell them as advertised; and

(d) Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

192. T-Mobile violated Civil Code § 1770, in the following ways:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and California Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and California Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Failing to timely and adequately notify Plaintiff and California Subclass members of the Data Breach;

(g) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and California Subclass members'

(h) Private Information; and

(i) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.*

193. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' Private Information.

194. Had T-Mobile disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, T-Mobile was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the California Subclass. T-Mobile accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because T-Mobile held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the California Subclass members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

195. As a direct and proximate result of T-Mobile's violations of California Civil Code § 1770, Plaintiffs and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information, including but not limited to the diminishment of their present and future property interest in their Private Information and the deprivation of the exclusive use of their Private Information.

196. Plaintiffs and the California Subclass have provided notice of their claims to T-Mobile, in compliance with California Civil Code § 1782(a), on the date of this filing. Plaintiffs and the California Subclass seek all relief allowed by law.

COUNT 11: CALIFORNIA CONSUMER PRIVACY ACT,

Cal. Civ. Code §§ 1798.100, *et seq.*

197. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges all preceding paragraphs, as if fully alleged herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer privacy.

198. Plaintiffs and California Subclass members are residents of California.

199. T-Mobile is a corporation that is organized or operated for the profit or financial benefit of its shareholders or other owners.

200. T-Mobile is a business that collects consumers' personal information as defined by Cal. Civ. Code § 1798.140(e). Specifically, T-Mobile obtains, receives, or accesses consumers' personal information when customers use T-Mobile's services.

201. T-Mobile uses consumers' personal data to provide services at customers' requests, as well as to develop, improve, and test T-Mobile's services.

202. T-Mobile violated Section 1798.150 of the California Consumer Privacy Act by failing to prevent Plaintiffs and the California Subclass members' nonencrypted and nonredacted

personal information from unauthorized access and exfiltration, theft, or disclosure as a result of T-Mobile's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

203. T-Mobile knew or should have known that its data security practices were inadequate to secure California Subclass members' Private Information and that its inadequate data security practices gave rise to the risk of a data breach.

204. T-Mobile failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the Private Information it collected and stored.

205. The cybercriminals accessed "nonencrypted and unredacted personal information" as covered by Cal. Civ. Code § 1798.81.5(A)(1)(d), in the Data Breach.

206. Upon information and belief, Plaintiff and California Subclass members' Private Information accessed by the cybercriminals in the Data Breach includes "nonencrypted and unredacted personal information" as covered by Cal. Civ. Code § 1798.81.5(A)(1)(d).

207. Plaintiffs seek injunctive relief in the form of an order requiring T-Mobile to employ adequate security practices consistent with law and industry standards to protect the California Subclass members' Private Information, requiring T-Mobile to complete its investigation, and to issue an amended statement giving a detailed explanation that confirms, with reasonable certainty, what categories of data were stolen and accessed without the California Subclass members' authorization, along with an explanation of how the data breach occurred.

208. As a direct and proximate result of T-Mobile's violations of the Cal. Civ. Code §§ 1798.150, Plaintiff and California Subclass members suffered damages, as described above.

209. On the date of this filing, counsel for the California Plaintiff served written notice identifying T-Mobile's violations of Cal. Civil Code § 1798.150(a) and demanding the data breach be cured, pursuant to Cal. Civil Code § 1798.150(b). If T-Mobile does not cure the noticed violation and provide Plaintiffs with an express written statement that the violations have been cured and that no further violations shall occur, Plaintiff and the California Subclass will seek statutory damages pursuant to Cal. Civil Code § 1798.150(a)(1)(A).

CLAIMS ON BEHALF OF THE HAWAII SUBCLASS

COUNT 12: HAWAII SECURITY BREACH NOTIFICATION ACT,

Haw. Rev. Stat. §§ 487N-1, *et seq.*

210. The Hawaii Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and alleges all preceding paragraphs, as if fully alleged herein. This claim is brought individually under the laws of Hawaii and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding security breach notification.

211. T-Mobile is a business that owns or licenses computerized data that includes "personal information" as defined by Haw. Rev. Stat. § 487N-2(a). Plaintiff and Hawaii Subclass members' Private Information includes "personal information" as covered under Haw. Rev. Stat. § 487N-2(a).

212. T-Mobile is required to accurately notify Plaintiff and Hawaii Subclass members if it becomes aware of a breach of its data security program without unreasonable delay under Haw. Rev. Stat. § 487N-2(a).

213. Because T-Mobile was aware of a breach of its security system, it had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Haw. Rev. Stat. § 487N-2(a).

214. By failing to disclose the Data Breach in a timely and accurate manner, T-Mobile violated Haw. Rev. Stat. § 487N-2(a).

215. As a direct and proximate result of T-Mobile's violations of Haw. Rev. Stat. § 487N-2(a), Plaintiff and Hawaii Subclass members suffered damages, as described above.

216. Plaintiff and Hawaii Subclass members seek relief under Haw. Rev. Stat. § 487N-3(b), including actual damages.

COUNT 13: HAWAII UNFAIR PRACTICES AND UNFAIR COMPETITION ACT,

Haw. Rev. Stat. §§ 480-1, *et seq.*

217. The Hawaii Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and alleges all preceding paragraphs, as

if fully alleged herein. This claim is brought individually under the laws of Hawaii and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding unfair practices and unfair competition.

218. Plaintiff and Hawaii Subclass members are "consumers" as defined by Haw. Rev. Stat. § 480-1.

219. Plaintiffs, the Hawaii Subclass members, and T-Mobile are "persons" as defined by Haw. Rev. Stat. § 480-1.

220. T-Mobile advertised, offered, or sold goods or services in Hawaii and engaged in trade or commerce directly or indirectly affecting the people of Hawaii.

221. T-Mobile engaged in unfair or deceptive acts or practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the goods and services purchased by Hawaii Subclass members in violation of Haw. Rev. Stat. § 480-2(a), including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Hawaii Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Hawaii Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass

members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Failing to timely and adequately notify Plaintiff and Hawaii Subclass members of the Data Breach;

(g) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Hawaii Subclass members'

(h) Private Information; and

(i) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

222. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' Private Information.

223. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Hawaii Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Hawaii Subclass members into believing they did not need to take actions to secure their identities.

224. T-Mobile intended to mislead Plaintiff and Hawaii Subclass members and induce them to rely on its misrepresentations and omissions.

225. The foregoing unlawful and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous.

226. T-Mobile acted intentionally, knowingly, and maliciously to violate Hawaii's Unfair Practices and Unfair Competition Act, and recklessly disregarded Plaintiff and Hawaii Subclass members' rights.

227. As a direct and proximate result of T-Mobile's deceptive acts and practices, Plaintiff and Hawaii Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including

from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

228. Plaintiff and Hawaii Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, benefit of the bargain damages, treble damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT 14: HAWAII UNIFORM DECEPTIVE TRADE PRACTICE ACT,

Haw. Rev. Stat. §§ 481A-3, *et seq.*

229. The Hawaii Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and alleges all preceding paragraphs, as if fully alleged herein. This claim is brought individually under the laws of Hawaii and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practice.

230. Plaintiff and Hawaii Subclass members are "persons" as defined by Haw. Rev. Stat. § 481A-2.

231. T-Mobile engaged in unfair and deceptive trade practices in the conduct of its business, violating Haw. Rev. Stat. § 481A-3, including:

(a) Representing that goods or services have characteristics that they do not have;

(b) Representing that goods or services are of a particular standard, quality, or grade if they are of another;

(c) Advertising goods or services with intent not to sell them as advertised; and

(d) Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

232. T-Mobile's unfair and deceptive trade practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Hawaii Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Hawaii Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Failing to timely and adequately notify Plaintiff and Hawaii Subclass members of the Data Breach;

(g) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Hawaii Subclass members' Private Information; and

(h) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

233. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' Private Information.

234. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Hawaii Subclass members, that their

LAW OFFICES
COTCHETT, PITRE & MCCARTHY, LLP

Cotchett, Pitre & McCarthy, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103

Private Information was not exposed and misled Plaintiffs and the Hawaii Subclass members into believing they did not need to take actions to secure their identities.

235. The above unfair and deceptive practices and acts by T-Mobile were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Hawaii Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

236. As a direct and proximate result of T-Mobile's unfair, unlawful, and deceptive trade practices, Plaintiff and Hawaii Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

237. Plaintiff and Hawaii Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, attorneys' fees and costs, and any other relief that the Court deems proper.

CLAIMS ON BEHALF OF THE WASHINGTON SUBCLASS

COUNT 15: WASHINGTON DATA BREACH NOTICE ACT,

Wash. Rev. Code §§ 19.255.010, *et seq.*

238. Plaintiffs repeat and allege all preceding paragraphs, as if fully alleged herein. This claim is brought individually under the laws of Washington and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding data breach notice.

239. T-Mobile is a business that owns or licenses computerized data that includes "personal information" as defined by Wash. Rev. Code § 19.255.010(1).

240. Plaintiffs and Washington Subclass members' Private Information includes "personal information" as covered under Wash. Rev. Code § 19.255.010(5).

241. T-Mobile is required to accurately notify Plaintiff and Washington Subclass members following discovery or notification of the breach of its data security program if Private

Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Private Information was not secured, in the most expedient time possible and without unreasonable delay under Wash. Rev. Code § 19.255.010(1).

242. Because T-Mobile discovered a breach of its security system in which Private Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Private Information was not secured, T-Mobile had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code § 19.255.010(1).

243. By failing to disclose the Data Breach in a timely and accurate manner, T-Mobile violated Wash. Rev. Code § 19.255.010(1).

244. As a direct and proximate result of T-Mobile's violations of Wash. Rev. Code § 19.255.010(1), Plaintiffs and Washington Subclass members suffered damages, as described above.

245. Plaintiffs and Washington Subclass members seek relief under Wash. Rev. Code §§ 19.255.040, including actual damages and injunctive relief.

COUNT 16: WASHINGTON CONSUMER PROTECTION ACT,

Wash. Rev. Code Ann. §§ 19.86.020, *et seq.*

246. Plaintiffs repeat and allege all preceding paragraphs as if fully alleged herein. This claim is brought individually under the laws of Washington and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

247. T-Mobile is a "person," as defined by Wash. Rev. Code Ann. § 19.86.010(1).

248. T-Mobile advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

249. T-Mobile engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Washington Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Washington Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Failing to timely and adequately notify Plaintiffs and Washington Subclass members of the Data Breach;

(g) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Washington Subclass members' Private Information; and

(h) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

250. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' Private Information.

251. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Washington Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Washington Subclass members into believing they did not need to take actions to secure their identities.

252. T-Mobile acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff and Washington Subclass members' rights.

253. T-Mobile's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, including, but not limited to Wash. Rev. Code §§ 19.255.010, et seq.. Alternatively, T-Mobile's conduct is injurious to the public interest because it has injured Plaintiff and Washington Subclass members, had the capacity to injure persons, and has the capacity to injure other persons, and has the capacity to injure persons. Further, its conduct affected the public interest, including the millions of Washingtonians affected by the Data Breach.

254. As a direct and proximate result of T-Mobile's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and Washington Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

255. Plaintiff and Washington Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their Counsel to represent the Class and Subclasses;

B. For equitable relief enjoining T-Mobile from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the class and Subclass members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and the class members or to mitigate further harm;

C. For equitable relief compelling T-Mobile to use appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of T-Mobile's wrongful conduct;

E. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

F. For an award of punitive damages, as allowable by law;

G. For an award of attorneys' fees and costs, and any other expense, including reasonable expert witness fees;

H. Pre- and post-judgment interest on any amounts awarded; and

I. Such other and further relief as this court may deem just and proper.

IX. JURY TRIAL DEMAND

Plaintiffs hereby demand a jury trial for all claims so triable.

Dated: August 23, 2021

Respectfully submitted,

COTCHETT, PITRE & McCARTHY, LLP

/s/ Karin B. Swope
Karin B. Swope

KARIN B. SWOPE (WSBA # 24015)
kswope@cpmlegal.com
COTCHETT, PITRE & McCARTHY, LLP
7511 Greenwood Avenue N, Suite 4057
Seattle, WA 98103
Telephone: (206) 778-2123

Facsimile: (650) 697-0577

ADAM J. ZAPALA (*pro hac vice* pending)
azapala@cpmlegal.com
ELIZABETH T. CASTILLO (*pro hac vice* pending)
ecastillo@cpmlegal.com
KAIYI A. ZIE (*pro hac vice* pending)
kzie@cpmlegal.com
REID W. GAA (*pro hac vice* pending)
rgaa@cpmlegal.com
COTCHETT, PITRE & McCARTHY, LLP
840 Malcolm Road
Burlingame, CA 94010
Telephone: (650) 697-6000
Facsimile: (650) 697-0577

Attorneys for Plaintiffs Crystal Lam and Nina Phan